

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-316963

(43)Date of publication of application : 29.11.1996

(51)Int.Cl.

H04L 12/28

G06F 15/00

H04L 9/32

H04L 12/24

H04L 12/26

(21)Application number : 07-115422

(71)Applicant : NEC CORP

(22)Date of filing : 15.05.1995

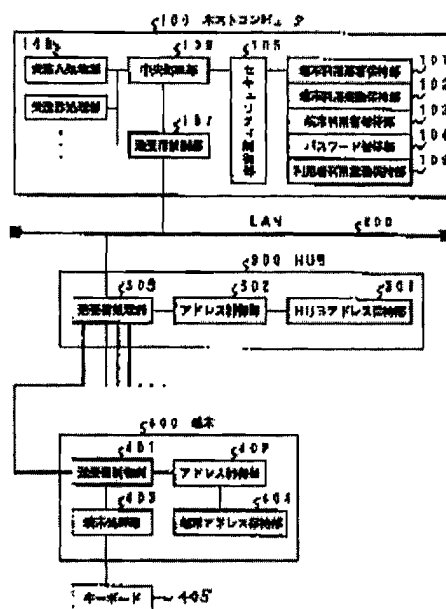
(72)Inventor : HARIKAWA KIKUNOSUKE

(54) TERMINAL SECURITY MANAGEMENT DEVICE

(57)Abstract:

PURPOSE: To prevent the wrong use by providing a host computer provided with a user's use application holding part, an application processing part, a central processing part, a security control part, and a transmission/reception control part and a HUB provided with a transmission/reception processing part.

CONSTITUTION: When receiving a start message from a central processing part 106, a security control part 105 checks a user ID and a password holding part 104 to confirm whether the user has the right to the use or not and to identify the user. Next, the control part 105 compares a use application number and a user's use application holding part 109 to confirm whether the user has the right of the use of the application or not and retrieves a terminal user holding part 103 by a terminal address and the user ID to confirm whether the user has the right of the use of the terminal or not. Next, the control part 105 retrieves a terminal's use application holding part 102 by the terminal address and the use application number to confirm whether the terminal has the right of the use or not and retrieves a terminal use place holding part 101 by the terminal address and a HUB address to confirm whether the terminal is used under a correct HUB or not.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-316963

(43) 公開日 平成8年(1996)11月29日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/28			H 0 4 L 11/00	3 1 0 Z
G 0 6 F 15/00	3 1 0	9364-5L	G 0 6 F 15/00	3 1 0 A
H 0 4 L 9/32			H 0 4 L 9/00	A
12/24		9466-5K	11/08	
12/26				

審査請求 有 請求項の数2 O L (全 6 頁)

(21) 出願番号 特願平7-115422

(22) 出願日 平成7年(1995)5月15日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 針川 菊之介

東京都港区芝五丁目7番1号 日本電気株式会社内

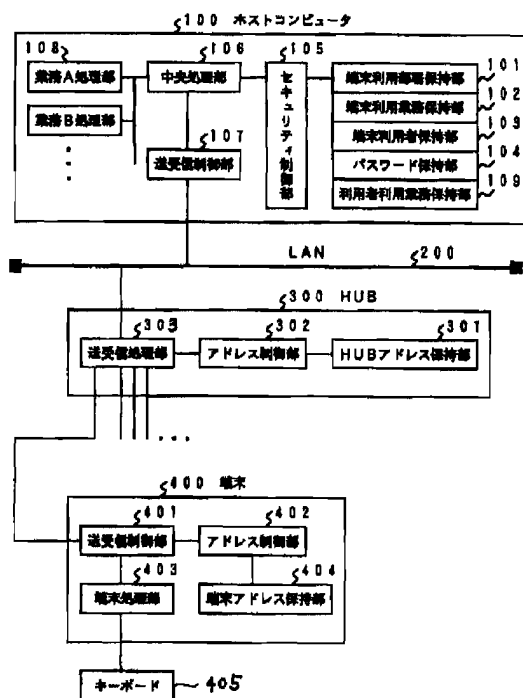
(74) 代理人 弁理士 後藤 洋介 (外2名)

(54) 【発明の名称】 端末セキュリティ管理装置

(57) 【要約】 (修正有)

【目的】 セキュリティ管理上パスワードにより利用者を確認できてもその利用者が悪意を持った場合にも不正利用を防止する。

【構成】 パスワード保持部104、セキュリティ制御部105、送受信制御部107を有するホストコンピュータ100と、端末400をLAN200に接続するための装置であり、LAN上のHUBを一意にするためのアドレスが格納されるHUBアドレス保持部301とアドレス制御部302と送受信処理部303を有するHUB300と、自分のアドレスを管理している端末アドレス保持部404とアドレス制御部402と送受信制御部401と端末処理部403と利用者のパスワード、処理業務、等を入力するキーボード405を有する端末400から成る。悪意の利用者が利用できる端末が限定され、その端末での業務も限定され、作業場所を限定される。



【特許請求の範囲】

【請求項 1】 端末毎にその端末が接続できる HUB のアドレスを管理している端末利用部署保持部と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部と端末毎にその端末を利用できる人を管理している端末利用者保持部と利用者 ID とその端末利用者が入力するパスワードを管理しているパスワード保持部と利用者が利用できる業務を管理している利用者利用業務保持部及び業務処理部、中央処理部、セキュリティ制御部、送受信制御部とを有するホストコンピュータと、端末を LAN に接続するための装置であり LAN 上の HUB アドレス保持部とそのアドレスを制御するアドレス制御部とデータの受け渡しを行う送受信処理部とを有する HUB と、自分のアドレスを管理している端末アドレス保持部とそのアドレスを処理するアドレス制御部とメッセージの送受信を行う送受信制御部と端末処理部と利用者のパスワード・処理業務等を入力する入力手段とを有する端末とから成ることを特徴とする端末セキュリティ管理装置。

【請求項 2】 請求項 1 記載の端末セキュリティ管理装置において、前記入力手段はキーボードにより構成されることを特徴とする端末セキュリティ管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は端末セキュリティ管理装置に関し、特に LAN によるオンライン処理のセキュリティ管理装置に関する。

【0002】

【従来の技術】 従来の端末セキュリティ管理装置は、図 2 に示すように、アクセス用の端末 1 及び第一のモデム 2 を持つアクセス用端末局側から第二のモデム 4 及び被アクセス用のデータベース 5 を持つセンター局側へのアクセス時に端末 1 から入力されたユーザ識別信号をセンター局側で受けて該ユーザのアクセス権の有無を照合し、アクセス権有りの場合に該アクセスを許可する方式において、前記第一のモデム 2 は、前記アクセス前に予め前記センター局側から発したモデム識別用の第二の識別信号を記憶し、前記アクセス時に前記センター局側から発した送信要求にตอบสนองして予め記載されているモデム識別用の第二の識別信号と予め別手段で与えられかつ前記端末 1 から入力される第二の識別信号とを照合し一致する場合、第二の識別信号を発生し返送するための識別信号を有し前記第二のモデム 4 は、前記アクセス時に前記送信要求を発した後返送されてくる前記第二の識別信号を受けて前記第一のモデム 2 のアクセス権の有無を照合するためのモデム識別信号照合手段を有し、前記第一及び第二の識別信号の両照合結果が共にアクセス権有りの場合にのみ該アクセスを許可するようになっている（特開昭 64-4138 号参照）。尚、図 2 において、

第一のモデム 2 は、端末インタフェース 20 と、送信回路 21 と、受信回路 22 と、ラインインタフェース 23 と、ID 照合・発生回路 24 とを有する。また、第二のモデム 4 は、端末インタフェース 40 と、送信回路 41 と、受信回路 42 と、ラインインタフェース 43 と、ID 照合・発生回路 44 とを有する。

【0003】 次に、図 2 に示した従来の端末セキュリティ管理装置の動作について説明する。ID 照合・発生回路 24 は、センター局から予めアクセス前に発信するモデム場所を識別する ID を記憶する ID メモリーを内蔵している。これは予めデータベース 5 に登録されている電話番号（即ち場所）から正しくアクセスがなされる事を保証するため、予めセンター局から各端末へダイヤルし、個々のモデム ID を送信する。各端末側のモデムは、前記 ID 照合・発生回路 24 のメモリー内に本モデム ID を記憶する。またセンター局から端末へ送信されるモデム ID と別に、同じモデム ID を別のルート（例えばメール等）で端末側へ知らされる。端末局からセンター局へのアクセス時には、端末局から発呼（ダイヤル）を行い、これに対するセンター局の自動応答により公衆電話網 3 での回線接続が完了する。この後センター局側の第二のモデム 4 が端末局に対して ID 照合・発生回路 44 によりモデム ID の送信要求を出す。この送信要求を受信した第一のモデム 2 は端末 1 に対してモデム ID 送信要求を出す。端末 1 は予め与えられたモデム ID（モデム 2 にロードされた ID とは別ルートでユーザに与えられている）を第一のモデム 2 へ入力する。第一のモデム 2 では予めメモリーされているモデム ID と比較／照合した後、合致していればモデム ID の送信を行う。これを受けたデータベース 5 は、アクセス権をもつ端末局のモデム ID であるか否かを逐一照合し、照合結果がアクセス権有りを示した時だけ肯定応答 ACK を端末局へ送信する。

【0004】

【発明が解決しようとする課題】 この従来のこの方式ではアクセス権確認のためには、端末からモデム ID を複数の人が使用する場合全員が同一のモデム ID を入力することになり、人毎のアクセス権の確認ができない。又、LAN の様に一つの通信回線で一カ所に複数の端末を設置する場合、端末毎にモデムを設置しなければならず HUB の様な機器（一つの機器で複数の端末を LAN に接続する機器）の場合は対応できないという問題がある。

【0005】

【課題を解決するための手段】 本発明によれば、端末毎にその端末が接続できる HUB のアドレスを管理している端末利用部署保持部と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部と端末毎にその端末を利用できる人を管理している端末利用者保持部と利用者 ID とその端末利用者が入力するパスワードを管

理しているパスワード保持部と利用者が利用できる業務を管理している利用者利用業務保持部及び業務処理部、中央処理部、セキュリティ制御部、送受信制御部とを有するホストコンピュータと、端末をLANに接続するための装置でありLAN上のHUBを一意にするためのアドレスが格納されているHUBアドレス保持部とそのアドレスを制御するアドレス制御部とデータの受け渡しを行う送受信処理部とを有するHUBと、自分のアドレスを管理している端末アドレス保持部とそのアドレスを処理するアドレス制御部とメッセージの送受信を行う送受信制御部と端末処理部と利用者のパスワード・処理業務等を入力する入力手段とを有する端末とから成ることを特徴とする端末セキュリティ管理装置が得られる。

【0006】また、本発明によれば、前記入力手段はキーボードにより構成されることを特徴とする端末セキュリティ管理装置が得られる。

【0007】

【実施例】次に、本発明の実施例に係る端末セキュリティ管理装置について図面を参照して説明する。

【0008】本実施例の端末セキュリティ管理装置は、図1に示すように、端末毎にその端末が接続できるHUB300のアドレスを管理している端末利用部署保持部101と端末毎にその端末で処理出来る業務を管理している端末利用業務保持部102と端末毎にその端末を利用できる人を管理している端末利用者保持部103と利用者IDとその端末利用者が入力するパスワードを管理しているパスワード保持部104と利用者が利用できる業務を管理している利用者利用業務保持部109及び業務A処理部108等の業務処理部、中央処理部106、セキュリティ制御部105、送受信制御部107を有するホストコンピュータ100と、端末400をLAN200に接続するための装置であるが、LAN上のHUBを一意にするためのアドレスが格納されているHUBアドレス保持部301とそのアドレスを制御するアドレス制御部302とデータの受け渡しを行う送受信処理部303を有するHUB300と、自分のアドレスを管理している端末アドレス保持部404とそのアドレスを処理するアドレス制御部402とメッセージの送受信を行う送受信制御部401と端末処理部403と利用者のパスワード、処理業務、等を入力するキーボード405を有する端末400から成る。

【0009】即ち、ホストコンピュータ100は端末利用部署保持部101と端末利用業務保持部102と端末利用者保持部103とパスワード保持部104と業務A処理部108等の業務処理部と中央処理部106とセキュリティ制御部105と送受信制御部107と利用者利用業務保持部109から成る。端末利用部署保持部101は端末毎に（端末アドレス毎に）その端末が接続できるHUB300のアドレスを管理しておりつまり、これによりその端末が使える部署が限定できる。端末利用業

務保持部102は端末毎に（端末アドレス毎に）その端末で処理出来る業務名を管理しており、これによりその端末で利用できる業務（処理範囲）を限定できる。端末利用者保持部103は端末毎に（端末アドレス毎に）その端末を利用できる人（利用者のID番号で個人を認識し、その個人のID番号は端末より入力される）を管理しており、これにより個人毎に利用できる端末を限定できる。パスワード保持部104は利用者毎に利用者IDと利用者の暗唱番号を管理しており、他人による個人IDの不正使用を防止する。利用者利用業務保持部109は利用者毎にその利用者が利用出来る業務を管理しており利用者が利用出来る業務を制限できる。セキュリティ制御部105はホストコンピュータで受け取ったセキュリティ情報をもとに端末利用部署保持部101、端末利用業務保持部102、端末利用者保持部103、パスワード保持部104及び利用者利用業務保持部109の情報を確認し利用権の妥当性確認を行う。

【0010】中央処理部106はホストコンピュータの全体処理を行う。送受信制御部107はLANとのデータ通信を行う。業務A処理部108等の業務処理部は、複数の各業務処理部から成り各端末との実際の業務処理を行う。

【0011】LAN200はデータ通信を行うための通信回線でありLAN上には一つのホストコンピュータと複数の端末接続用HABが接続される。

【0012】HUB300はLANに端末を接続するための装置で有り一つのHUBには複数の端末を接続することができる。また、HUBはHUBアドレス保持部301、アドレス制御部302及び送受信処理部303から成る。HUBアドレス保持部301は全体でHUBを一意に識別するためのアドレス（番号）が格納されており端末のオンライン開始時このアドレスがホストコンピュータに通知される、ホストコンピュータではこれにより端末がどこの部署（HUB配下）で使用されようとしているか知ることができる。アドレス制御部302は端末のオンライン開始時HUBアドレス保持部よりHUBのアドレスを入手しホストコンピュータへ通知する。送受信処理部303はLANと端末とのデータ通信を行うが端末がオンライン開始する場合はアドレス制御部302へHUBのアドレス取得を指示しその結果をホストコンピュータへ通知する役割もある。

【0013】端末400はホストコンピュータと業務処理用端末で、送受信制御部401、アドレス制御部402、端末処理部403、端末アドレス保持部404及びキーボード405からなる。送受信制御部401はHUBとのデータ通信を行う装置であるがHUBに対してデータを送信する場合はアドレス制御部402に対して端末アドレスの取得を指示し、その結果の端末アドレスをメッセージに付加し送信する。アドレス制御部402は送受信制御部401の指示に従い、端末アドレス保持部

404より端末アドレスを取得し送受信制御部401へ通知する。端末アドレス保持部404は全端末を一意に識別するためのアドレス(番号)が格納されており、このアドレスをホストコンピュータとの送受信メッセージに付加することによりホストコンピュータは端末を一意に識別できる。キーボード405は端末側でオンライン開始時は利用者ID、パスワード及びオンラインの利用業務を入力する。

【0014】次に動作について説明する。端末よりオンライン処理を行う場合まず端末400のキーボード405より利用者のID、パスワード及び利用したい業務を入力する。入力されたデータは端末処理部403でオンライン開始の送信メッセージとして送受信制御部401へ渡される。送受信制御部401はアドレス制御部402へ指示し端末アドレス保持部404より端末アドレスを入手し送信メッセージに端末アドレスを付加しHUB300へ渡す。

【0015】HUB300は送受信処理部303で端末400からのメッセージを受け取りオンライン開始メッセージかどうかの判断を行いオンライン開始メッセージであればアドレス制御部302へ指示しHUBアドレス保持部301よりHABアドレスを入手しオンライン開始メッセージのHUBアドレスを付加しLAN200へメッセージを送信する。

【0016】オンライン開始メッセージはLAN200を通りホストコンピュータ100へ通知される。

【0017】ホストコンピュータ100ではLAN200からのメッセージを送受信制御部107で受け取り中央処理部106へ渡す。中央処理部106はオンライン開始メッセージの場合そのメッセージをセキュリティ制御部105へ渡しオンライン利用権の可否判定を行う。可否判定の結果合格であれば業務A処理部108等の業務処理部に対してメッセージを渡し、以降端末400との業務処理がおこなわれる。不合格であれば、利用権なしのメッセージを送受信制御部107を介して端末400へ通知する。セキュリティ制御部105は中央処理部106よりオンライン開始メッセージを受け取ると、まずメッセージ中の利用者IDとパスワードによりパスワード保持部104を調べ利用者のオンライン利用権があるか又、パスワードにより利用者本人かどうか確認する。次にメッセージ中の利用業務番号と利用者利用業務保持部109とを比較しその利用者が指定した業務が利用できる権利があるか確認する。次にメッセージ中の端末アドレスと利用者IDにより端末利用者保持部103

を検索しその利用者がその端末の利用権があるかどうかを確認する。次に、メッセージ中の端末アドレスと利用業務番号により端末利用業務保持部102を検索しその端末で指定の業務の利用権があるか確認する。次にメッセージ中の端末アドレスとHUBアドレスにより端末利用部署保持部101を検索しその端末が正しいHUB配下(正しい部署)で使用されているか確認する。これらの確認がすべて正しい(OK)の場合にセキュリティ制御部105は中央処理部106に対して合格を通知し一つでも不正があれば不合格を通知する。

【0018】

【発明の効果】以上説明したように、本発明は、悪意を持った利用者であっても利用できる端末が限定され、その端末で利用できる業務も限定され、さらに作業できる場所が限定され、またその場所に管理者が居ることを考えれば基本的には不正利用を防止できるという効果を有する。

【図面の簡単な説明】

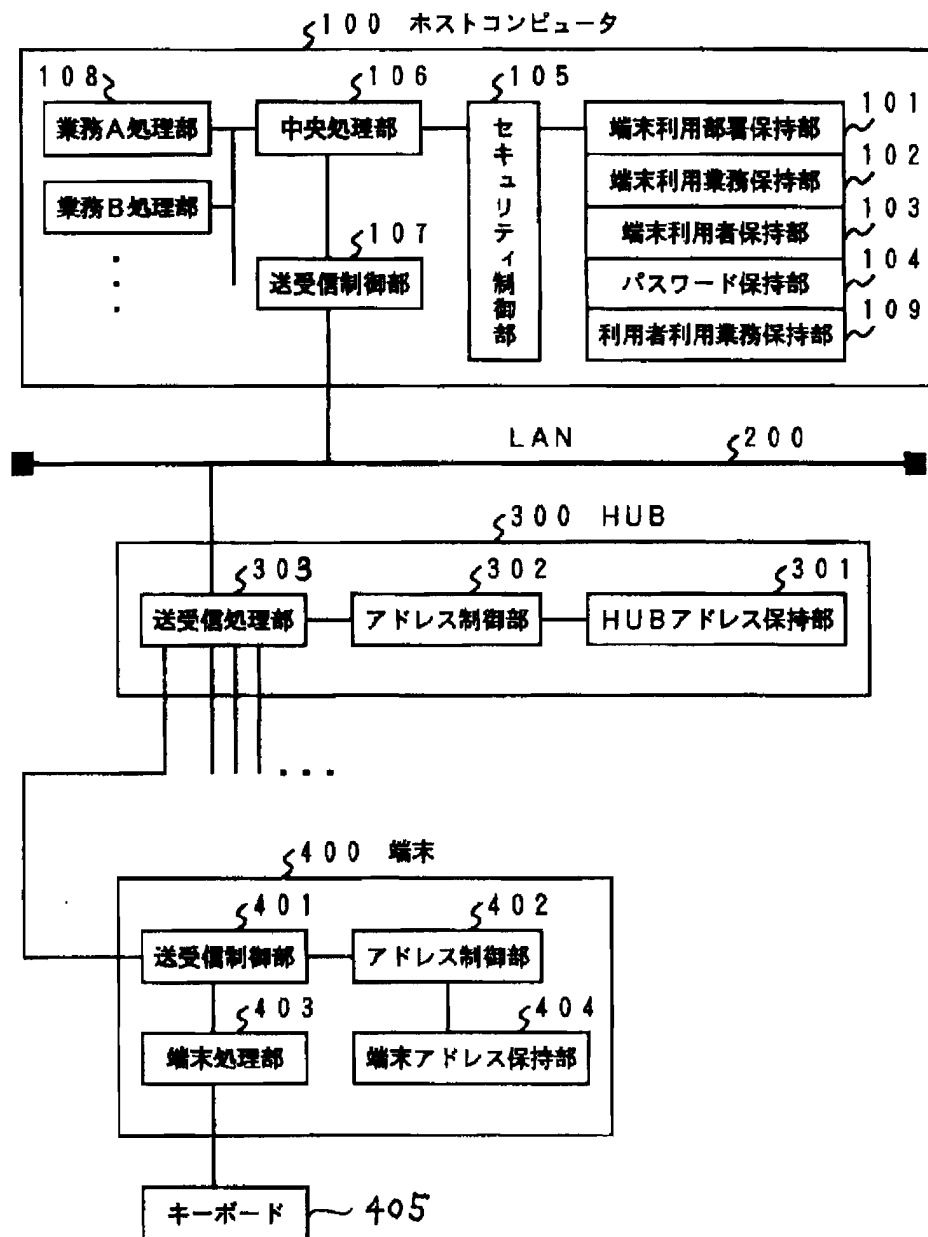
【図1】本発明の実施例に係る端末セキュリティ管理装置のブロック図である。

【図2】従来の端末セキュリティ管理装置のブロック図である。

【符号の説明】

100	ホストコンピュータ
101	端末利用部署保持部
102	端末利用業務保持部
103	端末利用者保持部
104	パスワード保持部
105	セキュリティ制御部
106	中央処理部
107	送受信制御部
108	業務A処理部
109	利用者利用業務保持部
200	LAN
300	HUB
301	HUBアドレス保持部
302	アドレス制御部
303	送受信処理部
400	端末
401	送受信制御部
402	アドレス制御部
403	端末処理部
404	端末アドレス保持部
405	キーボード

【図1】



【図2】

